

# Protocol for Direct Counterfactual Quantum Communication

Hatim Salih,<sup>1,\*</sup> Zheng-Hong Li,<sup>1,2</sup> M. Al-Amri,<sup>1,2</sup> and M. Suhail Zubairy<sup>1,2</sup>

<sup>1</sup>*The National Center for Mathematics and Physics,  
KACST, P.O.Box 6086, Riyadh 11442, Saudi Arabia*

<sup>2</sup>*Institute for Quantum Science and Engineering (IQSE) and Department of Physics and Astronomy,  
Texas A&M University, College Station, Texas 77843-4242*

(Dated: April 25, 2013)

It has long been assumed in physics that for information to travel between two parties in empty space, “Alice” and “Bob”, physical particles have to travel between them. Here, using the “chained” quantum Zeno effect, we show how, in the ideal asymptotic limit, information can be transferred between Alice and Bob without any physical particles traveling between them.

PACS numbers: 03.67.Hk, 03.67.-a, 03.65.Ta, 03.67.Dd, 03.67.Ac

Quantum mechanics has enjoyed immense success since its inception about a century ago. Its conceptual foundation, however, is often a matter of intense debate. Furthermore, several novel phenomena are predicted and observed based on quantum mechanics that appear counterintuitive and are unexplainable in the classical domain. Whole new fields owe their existence to this body of knowledge. One such field is quantum communication. In this paper we propose a surprising mode of communication whereby no physical particles travel between sender and receiver.

In 1970, the idea of “quantum money” [1]- money that cannot be forged - came to light, effectively kick-starting the field of quantum information. The idea, too advanced for its time, rested on the conjecture that quantum states cannot be faithfully copied, which was later proved as the no-cloning theorem [2]. Moreover, the mere act of measurement of an unknown quantum state alters it irreversibly. While “quantum money” has not turned out to be practical, the basic concept found direct application in cryptography [3–5] or, more precisely in quantum key distribution (QKD)[6–9]. The two most celebrated QKD protocols, the BB84 [6, 7] and E-91[8], both utilize basic ingredients from “quantum money” including that of a qubit.

Based on interaction-free measurements, or quantum interrogation [10–14], a QKD protocol was proposed [15] which left the door open for a more recent one employing the idea of counterfactuality, meaning no information-carrying qubits need to travel between Alice and Bob [16] - even though photons in this case can still be found in the transmission channel half the time on average (assuming a 50-50 beam splitter is used). This protocol was recently realized experimentally [17–19]. One drawback - apart from being nondeterministic - is that, even in the ideal case, only 12.5% of photons used are retained; the rest are discarded.

The basic idea of interaction-free measurement, central to both counterfactual cryptography and counter-

factual computation [20, 21], makes use of the fact that the presence of an obstructing object, acting as a measuring device, inside an interferometer setting, destroys interference even if no particle is absorbed by the object. This has the surprising consequence that sometimes the presence of such an object can be inferred without the object directly interacting with any (interrogating) particles. Using the quantum Zeno effect [22–27] (which refers to the fact that repeated measurement of an evolving quantum system can inhibit its evolution, leaving it in its initial state, an effect often paraphrased as “a watched kettle never boils”), the efficiency of such interaction-free measurements can be dramatically boosted.

Here, we take the logic of counterfactual communication to its natural conclusion. We show how in the ideal limit, using a chained version of the Zeno effect [23], information can be directly exchanged between Alice and Bob with no physical particles traveling between them, thus achieving direct counterfactual communication.

Our proposed setup is shown in Fig. 1. At Alice’s end, it is composed of two parts. The first part consists of a light source ( $S$ ) that sends a stream of horizontally polarized (H) photons, detectors ( $D_1$ ,  $D_2$  and  $D_3$ ), and a polarizing beam splitter  $PBS_0$  which only reflects vertically polarized photons V (as do all the  $PBS$  in the figure). The second part comprises two tandem Michelson interferometers. It includes two  $PBS$ s, two switchable polarization rotators ( $SRPs$ ), two switchable mirrors ( $SMs$ ) that can be switched on and off by external means, and two normal mirrors ( $MRs$ ). This part of the setup allows the signal photon to have a very large probability of staying at Alice’s end. On the other side, at Bob’s end, with the help of pockel cell  $PC_B$ , he can either switch the polarization of the incoming H photon to a V photon or keep the polarization state H unchanged. The  $PBS_B$  reflects V photons to a detector  $D_4$  (effectively blocking the communication channel) and allows H photons to be reflected back by the mirror  $MR_B$ . Bob can send a stream of logic 0’s and 1’s by either keeping the polarization state H unchanged (logic 0) or switching it to polarization state V (logic1). Bob’s choice of logic 0 and 1 leads to a click at detectors  $D_1$  and  $D_2$ , respectively with almost unit probability and with almost

---

\* salih.hatim@gmail.com

no photon in the transmission channel, thus leading to direct counterfactual communication.

This setup is implementable using current technology. However, before explaining how the setup works, we discuss an equivalent Mach-Zehnder type setup shown in Fig. 2, which helps us to understand the working principle of our protocol. In the Mach-Zehnder setup,  $BS$  stands for beam splitter. Initially, a photon is sent by Alice from the left such that the input state (before the top beam splitter) is  $|10\rangle$ . The state transformation at the beam splitters is described by  $|10\rangle \rightarrow \cos\theta|10\rangle + \sin\theta|01\rangle$  and  $|01\rangle \rightarrow \cos\theta|01\rangle - \sin\theta|10\rangle$ , where  $\cos\theta = \sqrt{R}$  with  $R$  being the reflectivity of the  $BS$ .

At Bob's end, ideal switches ( $SW$ ) allow Bob to pass the photon (logic 0) or to block it (logic 1).

We now show how to build a direct communication system using the quantum Zeno effect, which refers to the fact that repeated measurement of a gradually evolving quantum state leaves it unchanged.

Our purpose can be achieved in two steps. In the first step [see Fig.2(a)], we use a large number ( $N$ ) of beam splitters with a very small transmissivity, i.e.,  $\theta = \pi/2N$ . When Bob allows Alice's photon to pass, by switching off all  $SW$ s at his end, the initial state  $|10\rangle$  evolves coherently. After  $n$  cycles, the state of the photon can be written as

$$|10\rangle \rightarrow \cos n\theta|10\rangle + \sin n\theta|01\rangle. \quad (1)$$

Thus, at the end of  $N$  cycles ( $n = N$ ), the final state is  $|01\rangle$  and the detector  $D_2$  clicks. On the other hand, if Bob blocks the photon by switching on all  $SW$ s, the photonic state after  $n$  cycles is

$$|10\rangle \rightarrow \cos^{n-1}\theta(\cos\theta|10\rangle + \sin\theta|01\rangle) \approx |10\rangle, \quad (2)$$

where we assumed  $N$  to be large and  $\cos^N\theta \approx 1$ . Here the square of the overall factor ( $\cos^{2(n-1)}\theta$ ) represents the probability of having the state  $|10\rangle$  after  $n-1$  cycles. In this case the photon is reflected and the detector  $D_1$  clicks.

As a result, Bob's blocking causes detector  $D_1$  to click, while passing the photon causes detector  $D_2$  to click. This means that, in the ideal limit, Alice can read Bob's bit choices with arbitrarily large efficiency. This is the first step towards direct counterfactual quantum communication.

Although the Mach-Zehnder set-up, shown in Fig. 2(a), enables direct communication, the protocol is only partially counterfactual. In the case when Bob does not block, the photon's final state  $|01\rangle$  implies that the photon passes through the transmission channel with unit probability at  $N$ -th cycle.

We now present a protocol that leads not only to direct communication between Alice and Bob but is also fully counterfactual. We use the chained version of the quantum Zeno effect, as shown in Fig.2(b). The signal photon passes through " $M$ " big cycles separated by  $BS_M$ s with  $\theta_M = \pi/2M$ . For the  $m$ th cycle ( $m \leq M$ ), there are " $N$ " beam splitters  $BS_N$ s with  $\theta_N = \pi/2N$ .

We assume that initially Alice sends a single photon as shown in Fig. 2(b), where all unused ports are in the vacuum state. As a result of beam splitter transformations, now we have three photon states  $|i, j, k\rangle$ ; where  $|i\rangle$ ,  $|j\rangle$ , and  $|k\rangle$  correspond to the photon states at the left-hand side arms of the outer chain, at the left-hand side arms of the inner chain, and at the right-hand side arms of the inner chain, respectively. By using the results shown in Eqs. (1) and (2), it is easy to see that if Bob passes Alice's photon, for the  $m$ -th cycle, we have

$$|010\rangle \rightarrow \cos n\theta_N|010\rangle + \sin n\theta_N|001\rangle \xrightarrow{n=N} |001\rangle. \quad (3)$$

The initial state of the total system is  $|100\rangle$ . We can see the evolution by including results from Eqs. (1) and (2).

First we consider the case when Bob does not block at any stage (logic 0). After the  $m$ -th cycle, the resulting photon state is

$$|100\rangle \rightarrow \cos^{m-1}\theta_M(\cos\theta_M|100\rangle + \sin\theta_M|010\rangle) \xrightarrow{m=M} |100\rangle. \quad (4)$$

It is clear that after  $M$  big cycles and  $N$  small cycles detector  $D_1$  clicks. A click at the detector  $D_1$  ensures counterfactuality as any photon in the transmission channel would lead to a click at one of the detectors  $D_3$  [see Eq. (1)]. The probability of click at  $D_1$  is obtained by collecting all the contributions that are reflected from all the beam splitters  $BS_m$ 's and is given by  $P_1 = \cos^{2M}\theta_M$ .

On the other hand, if Bob blocks throughout (logic 1), we have (for the  $m$ -th cycle)

$$|010\rangle \rightarrow \cos^{n-1}\theta_N(\cos\theta_N|010\rangle + \sin\theta_N|001\rangle) \xrightarrow{n=N} |010\rangle, \quad (5)$$

where we assume  $N \gg 1$ . After the  $m$ -th cycle, the photon state is

$$|100\rangle \rightarrow \cos m\theta_M|100\rangle + \sin m\theta_M|010\rangle \xrightarrow{m=M} |010\rangle. \quad (6)$$

Thus after  $M$  big cycles and  $N$  small cycles, detector  $D_2$  clicks. Again counterfactuality is ensured by a click at  $D_2$  as any photon in the transmission channel would be absorbed by the blocking device and would not be available for detection at  $D_2$ . The probability of click at the detector  $D_2$  is given by  $P_2 = |y_{\{M,0\}}|^2$ , where  $y_{\{M,0\}}$  can be obtained from the recursion relations  $x_{m+1} = a_M x_m - b_M y_{\{m,N\}}$ ,  $y_{\{m+1,0\}} = b_M x_m + a_M y_{\{m,N\}}$ ,  $y_{\{m,n\}} = a_N y_{\{m,n-1\}} - b_N z_{\{m,n-1\}}$  and  $z_{\{m,n\}} = c(b_N y_{\{m,n-1\}} + a_N z_{\{m,n-1\}})$  where  $a_{N(M)} = \cos\theta_{N(M)}$ ,  $b_{N(M)} = \sin\theta_{N(M)}$ , and  $c = 0$  with  $x_1 = a_M$ ,  $y_{\{1,0\}} = b_M$  and  $z_{\{m,0\}} = 0$ . Obviously, if  $c = 1$ , we can get the probability  $D_1$  clicking ( $P_1 = |x_M|^2$ ) for the case Bob encoding "0".

We emphasize that for  $D_1$  or  $D_2$  clicking, no photon could have passed through the transmission channel, since the presence of any photon in the channel would

have led to detection events at  $D_3$  (for Bob does not block) or at Bob's blocking device (for Bob blocks).

In Figs. (3a) and (3b), we have plotted the probabilities  $P_1$  and  $P_2$  by using the above recursion relations. It is clearly seen that  $P_1$  is above 0.90 for  $M > 25$  and is independent of  $N$ ; however, a value of  $P_2$  above 0.90 requires a much larger value of  $N$ . Our numerical estimates indicate ( $P_1 = 0.906$ ,  $P_2 = 0.912$ ) for ( $M = 25$ ,  $N = 320$ ); ( $P_1 = 0.952$ ,  $P_2 = 0.953$ ) for ( $M = 50$ ,  $N = 1250$ ), and ( $P_1 = 0.984$ ,  $P_2 = 0.982$ ) for ( $M = 150$ ,  $N = 10000$ ). This shows that perfect counterfactuality is possible, albeit for large values of  $M$  and  $N$ .

This may be complicated for the Mach-Zehnder setup discussed so far. However a Michelson interferometer-based implementation offers significant practical advantages. Thus, after elucidating the essential features of our direct counterfactual quantum communication protocol, we revert to a discussion of the Michelson-type configuration shown in Fig. 1. This allows a better practical realization of the protocol, with a massive saving of resources.

Here, the function of  $BS$  is replaced by the combination of  $PBS$  and  $SPR$ . Assume the state of an H photon is  $|H\rangle$ , and the state of a V photon is  $|V\rangle$ . Then, each time the photon passes through one  $SPR$ , the polarization evolves as follows  $|H\rangle \rightarrow \cos \beta_i |H\rangle + \sin \beta_i |V\rangle$  and  $|V\rangle \rightarrow \cos \beta_i |V\rangle - \sin \beta_i |H\rangle$ , where  $\beta$  represents the rotation angle with the subscript  $i = 1, 2$  corresponding to different  $SPRs$ . The mirror  $SM_{1(2)}$  is switched off initially to allow the photon to be transmitted but it remains on during  $M(N)$  cycles and is turned off again after  $M(N)$  cycles are completed. The initial photon emitted by the light source is  $|H\rangle$ . Since the signal photon passes through  $SMs$  twice each cycle, we set  $\beta_{1(2)} = \pi/4M(N)$ . It is not difficult to see that if Bob blocks the photon, detector  $D_2$  clicks. Also, if Bob passes the photon, detector  $D_1$  clicks.

Next we consider the effect of imperfections of the system and noise in the transmission channel on the performance of counterfactual communication. There are two kinds of imperfections: The first one only affects the efficiency of communication, but does not cause measurement errors. Imperfection coming from the sensitivity of detectors  $D_1$  and  $D_2$  is an example of this. If the sensitivity of these detectors is  $\eta$ , then the efficiency of communication also reduces to  $\eta$ . However, the second kind of imperfection, which mainly comes from the switchable polarization rotators ( $SPRs$ ), results in measurement errors. During each cycle,  $SPRs$  should rotate the signal photon with a certain angle, but in practical situations there can be a slight error in the angle. Let us suppose that the error for the  $SPR$  in the inner cycle is  $\Delta\theta_{N=s_N}(\theta_N/N)$ ; namely, the photon state is rotated with an additional angle  $s_N\theta_N$  after  $N$  cycles. The corresponding coefficient for the error of the  $SPR$  in the outer cycle is  $s_M$ . We can estimate their influence numerically by replacing  $\theta_{N(M)}$  with  $\theta_{N(M)} + \Delta\theta_{N(M)}$  for fixed  $N$  and  $M$  in the recursion relations given above. In

Fig. 4(a), we plot the detector successful clicking rates for different values of  $s$  (setting  $s = s_N = s_M$ ). It is clear that the performance is still good if the factor  $s$  is less than two. In Fig. 4, we also show the error rate associated with the wrong clicking of  $D_1$  and  $D_2$  by using the concept of mutual information  $I(X, Y)$ . We consider a communication process in which Bob sends messages composed of logic 0 and 1 with equal probabilities. Let the ensemble 'X' represent the detector 'x' clicking, with  $x = D_1, D_2, D_3, D_4$ . Also the events  $y \in Y$  correspond to the clicking of detectors  $D_1$  and  $D_2$  giving wrong information; i.e.,  $y = D_1$  represents Bob sending "1" (Alice's  $D_1$  incorrectly clicking instead of  $D_2$ ) and  $y = D_2$  represents Bob sending "0" (Alice's  $D_2$  incorrectly clicking instead of  $D_1$ ). Then, mutual information can be defined as

$$I(X, Y) = \sum_{x, y} P(x, y) \log \frac{P(x, y)}{P(x)P(y)} \quad (7)$$

$$= - \sum_{i=1,2} P(y = D_i) \log P(x = D_i)$$

It is easy to see that if the error rate is zero, the mutual information is zero.

Another source of noise results when the transmission channel is blocked by an object other than Bob's. We can define the noise rate as  $B$ . This represents the probability of any object other than Bob's blocking the channel. It is easy to see if Bob chooses to block his path, the result at Alice's end does not change. For the case when Bob allows the photon component to be reflected, the result again does not change appreciably if there is blocking only in one cycle. However, the noise may cause a problem if blocking takes place in multiple cycles. In Fig. 4(b), we plot the probability of  $D_1$  clicking for different values of  $B$  as well as the mutual information. To simulate the noise, we create random numbers between 0 and 1 each time the photon component passes through the transmission channel. If the number is less than  $B$ , we take the transmission channel to be blocked (set  $c = 0$  for that cycle, otherwise  $c = 1$ ). The figure shows that the blocking rate  $B$  should be suppressed under 0.2%. A higher loss may adversely affect our protocol.

We also note that the time control of switchable mirrors ( $SMs$ ) is also very important. Suppose the distance between Alice and Bob is  $L$ . The control time of these switchable mirrors should be less than  $2L/c_0$  ( $c_0$  being the light speed).

In summary, we strongly challenge the longstanding assumption that information transfer requires physical particles to travel between sender and receiver by proposing a direct quantum communication protocol whereby, in the ideal asymptotic limit, no photons pass through the transmission channel, thus achieving complete counterfactuality. In so doing we highlight the essential difference between classical and quantum information.

## ACKNOWLEDGMENTS

This research is supported by a grant from King Abdulaziz City for Science and Technology (KACST) and

an NPRP grant (4-520-1-0830) from Qatar National Research Fund (QNRF).

- 
- [1] S. Wiesner, SIGACT News **15** 78 (1983).
  - [2] W.K. Wootters and W.H. Zurek, Nature **299** 802 (1982).
  - [3] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Fourth Estate, London 1999).
  - [4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74** 145 (2002)
  - [5] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948); *ibid.* **27**, 623 (1948); *ibid.* **28** 656 (1949).
  - [6] C. H. Bennett, and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, (IEEE, New York 1984), p.175.
  - [7] C. H. Bennett and G. Brassard, 1985, IBM Tech. Discl. Bull. **28**, 3153 (1985).
  - [8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
  - [9] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
  - [10] A. C. Elitzur, and L. Vaidman, Found. Phys. **23**, 987 (1993).
  - [11] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, Phys. Rev. Lett. **74**, 4763 (1995).
  - [12] N. Namekata and S. Inoue, J. Phys. B **39**, 3177 (2006).
  - [13] J. S. Jang, Phys. Rev. A **59**, 2322 (1999).
  - [14] R. H. Dicke, Am J. Phys, **49** 925 (1981).
  - [15] G-C. Guo and B-S. Shi, Phys. Lett. A **256**, 109 1999
  - [16] T.-G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).
  - [17] M. Ren, G. Wu, E. Wu, and H. Zeng, Laser Phys. **21**, 755 (2011).
  - [18] G. Brida, A. Cavanna, I.P. Degiovanni, M. Genovese, P. Traina, Laser Phys. Lett. **9**, 247 (2012).
  - [19] Y. Liu, L. Ju, X. L. Liang, S. B. Tang, Guo-LiangShen Tu, L. Zhou, C. Z. Peng, K. Chen, T. Y. Chen, Z. B. Chen, and J. W. Pan, Phys. Rev. Lett. **109**, 030501 (2012).
  - [20] R. Jozsa, in *Lecture Notes in Computer Science*, edited by C. P. Williams (Springer-Verlag, Berlin 1999), p. 1509.
  - [21] G. Mitchison and R. Jozsa, Proc. R. Soc. A **457**, 1175 (2001).
  - [22] P. G. Kwiat, A. G. White, J. R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. **83**, 4725 (1999).
  - [23] O. Hosten, M. T. Rakher, J. T. Barreiro, N. A. Peters, and P. G. Kwiat, Nature (London) **439**, 949 (2006).
  - [24] P. G. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, in *Fundamental Problems in Quantum Theory: A Conference Held in Honor of Professor John A. Wheeler*, Annals of the New York Academy of Sciences (New York Academy of Sciences, New York, 1995), vol. 755.
  - [25] B. Misra and E. C. G. Sudarshan, J. Math. Phys **18**, 756 (1977).
  - [26] A. Peres, Am. J. Phys. **48**, 931 (1980).
  - [27] G. S. Agarwal and S. P. Tewari, Phys. Lett. A **185**, 139 (1994).

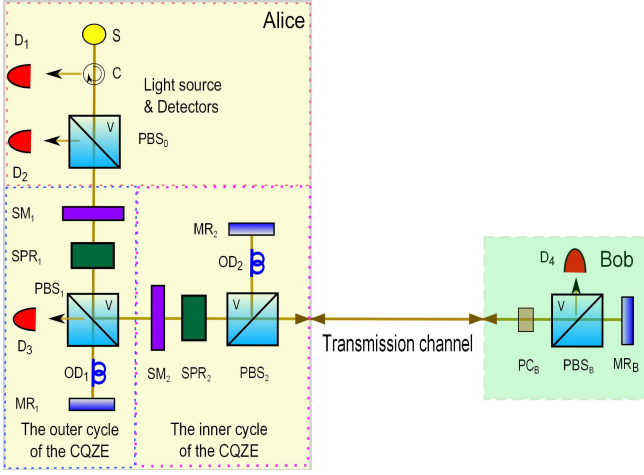


FIG. 1. (Color online) In the figure,  $S$  stands for the light source,  $C$  is the optical circulator,  $D_1$ ,  $D_2$ ,  $D_3$  and  $D_4$  are photon detectors,  $PBS$  stands for polarizing beam splitter which only reflects vertically polarized photons (V),  $SPR$  stands for switchable polarization rotator,  $PC$  stands for Pockels cell that determines the polarization state of the transmitted photons,  $SM$  stands for switchable mirror,  $MR$  stands for a normal mirror and  $OD$  stands for optical delay. Only horizontally polarized photons (H) will be sent into the tandem Michelson interferometers. The two optical paths  $SM_1 \rightarrow MR_1$  and  $SM_1 \rightarrow MR_B$  for the first Michelson interferometer correspond to the outer cycle of the chained quantum Zeno effect CQZE ( $M$  cycles) for Mach-Zehnder setup, while the paths  $SM_2 \rightarrow MR_2$  and  $SM_2 \rightarrow MR_B$  for the second Michelson interferometer, correspond to the inner cycle of the CQZE ( $N$  cycles). The mirror  $SM_{1(2)}$  is switched off initially to allow the photon to be transmitted but it then remains on for  $M(N)$  cycles, and is turned off again after  $M(N)$  cycles are completed. Here  $SPR_{1(2)}$  rotates the polarization by a small angle  $\beta_{M(N)} = \pi/4M(N)$  (for each cycle, the photon passes  $SPR$  twice), i.e.,  $|H\rangle$  evolves to  $\cos \beta_{M(N)} |H\rangle + \sin \beta_{M(N)} |V\rangle$  and  $|V\rangle$  evolves to  $\cos \beta_{M(N)} |V\rangle - \sin \beta_{M(N)} |H\rangle$ .  $OD_1$  and  $OD_2$  guarantee that optical distances of different paths of same interferometer exactly match. At Bob's end, Bob passes an H photon by turning off his  $PC$  reflecting it back, and he blocks an H photon by turning on his  $PC$ , changing the photon's polarization to V. We emphasize that the chance of Alice's photon leaking into the transmission channel is almost zero for large enough  $M$  and  $N$ .



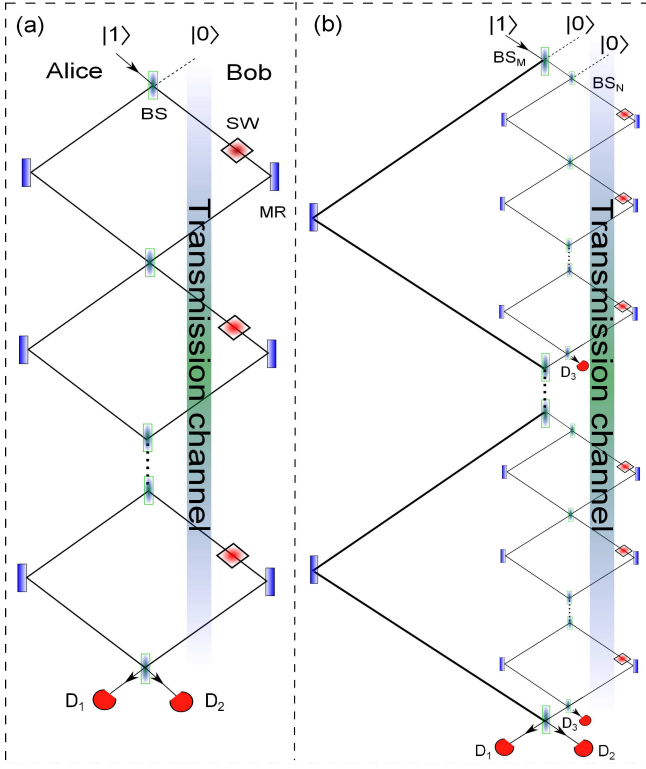


FIG. 2. (Color online) Here  $BS$  stands for beam splitter and  $SW$  stands for ideal switches. In the transmission channel, the photon is accessible to Eve. (a) The  $BS$ s have large reflectivity,  $R = \cos^2\theta = \cos^2(\pi/2N)$  with  $N$  being the total number of beam splitters. (b) By using a chained version of the setup shown in (a), we can achieve direct counterfactual quantum communication. Two kinds of  $BS$ s are used. One is  $BS_M$  for  $M$  big cycles. The other is  $BS_N$  for  $N$  small cycles within each  $M$  cycle. There are a total of  $M \times N$  cycles for one signal. As discussed in the text, the probability of finding a signal photon in the transmission channel is nearly zero. Clicks at  $D_1$  or  $D_2$  reveal to Alice Bob's bit choices.

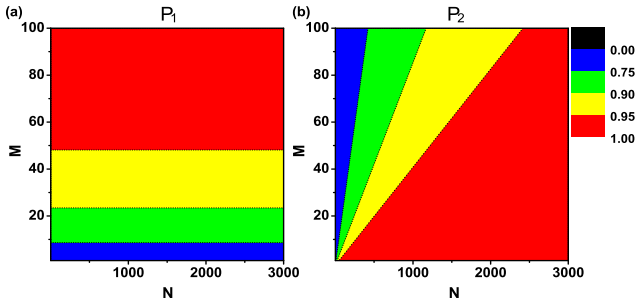


FIG. 3. (Color online)  $P_1$  and  $P_2$ , which are the probabilities of  $D_1$  and  $D_2$  clicking, respectively, are plotted against different number of cycles  $M$  and  $N$  for (a) Bob unblocking Alice's photon and (b) Bob obstructing Alice's photon.

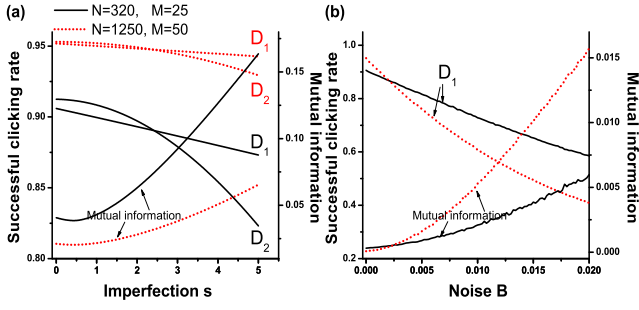


FIG. 4. (Color online) (a) The variation of the rate of successful clicking plotted for  $D_1$  and  $D_2$  as a function of  $s$ , where  $s$  describes the imperfection of the switchable polarization rotators. Also plotted is the mutual information describing the error rate of  $D_1$  and  $D_2$  as a function of  $s$ . (b) The rate of successful clicking of  $D_1$  and the corresponding mutual information both plotted as a function of noise  $B$ , defined as the probability of any object other than Bob's blocking the transmission channel. The red dotted curves are plotted for the case  $M=50, N=1250$ . The black solid curves are plotted for the case  $M=25, N=320$ .